

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
27 December 2002 (27.12.2002)

PCT

(10) International Publication Number
WO 02/103597 A1

(51) International Patent Classification⁷: **G06F 17/60**

(21) International Application Number: **PCT/KR02/01159**

(22) International Filing Date: **19 June 2002 (19.06.2002)**

(25) Filing Language: **Korean**

(26) Publication Language: **English**

(30) Priority Data:
2001/34886 20 June 2001 (20.06.2001) **KR**

(71) Applicant (for all designated States except US): **NITGEN CO., LTD.** [KR/KR]; 18th Fl. Korea Sanhak Research, Foundation Bldg, 1337-31, Seocho-Dong, Seocho-Gu, Seoul 137-070 (KR).

(72) Inventors; and

(75) Inventors/Applicants (for US only): **JUNG, Soon-Won** [KR/KR]; 1-1105 Jamwonhanshin, Apartment, 56-3

Jamwon-Dong, Seocho-Gu, Seoul 137-796 (KR). **LEE, Dong-Won** [KR/KR]; 112-402 Hyundae Apartment, 700-1(1/18) Poongdukchun-Ri, Suji-Eup, Yongin, Gyeonggi 449-846 (KR).

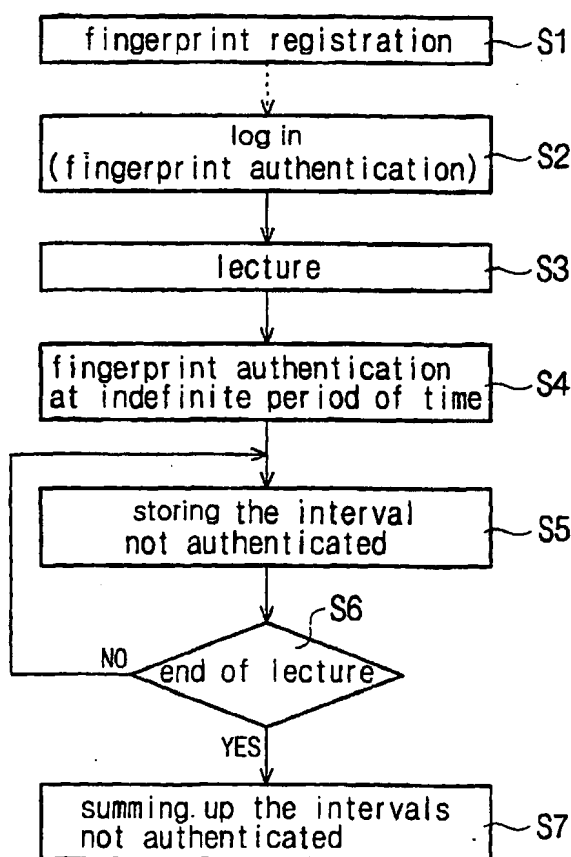
(74) Agent: **PARK, Sungmin**; 3F Dongbo Bldg, 647-8, Yoksam-dong, Gangnam-Gu, Seoul 135-080 (KR).

(81) Designated States (national): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZM, ZW.

(84) Designated States (regional): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM),

[Continued on next page]

(54) Title: **METHOD OF ATTENDANCE MANAGEMENT BY USING USER AUTHENTICATION ON ONLINE EDUCATION SYSTEM**



(57) Abstract: There is provided a method of attendance management by using user authentication on an online education system, which is realized on the online system composed of a plurality of clients, a plurality of education servers having user DBs, and an authentication server for authenticating the client to give him or her authority to be able to access the education servers by using biometric information (fingerprints, the iris, the retina, etc.), comprises the steps of: registering the client's biometric information in the authentication server; the client's logging in the education server through the authentication of the authentication server; and re-authenticating the client while the online lecture goes on.

WO 02/103597 A1



European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

— before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments

Published:

— with international search report

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

METHOD OF ATTENDANCE MANAGEMENT BY USING USER AUTHENTICATION ON ONLINE EDUCATION SYSTEM

5

Technical Field

The present invention relates to a method of attendance management by using user authentication on an online education system. More particularly, the present invention relates to a method which carries on efficient attendance management via user authentication in an online education system that students log in an education server and
10 take lessons therefrom on a network like the Internet.

Background Art

Recently, remote education systems are widely spread throughout the networks like LAN or the Internet which are developed through rapidly progressing Information
15 Technology like a computer, communication devices, communication media and digital technique. The remote education system has an advantage of overcoming the limits of time, distance and cost, but also has a disadvantage in that whether students are faithful to the lecture cannot be checked because the teacher and the students are remotely located.

Generally, only authenticated users can be accessible to the almost all online
20 education systems, and fingerprint is widely used as authenticating means. Fig. 1 and Fig. 2 show the examples of the fingerprint authentication systems on the Internet which can be regarded as a good representative of the network system.

Referring to Fig. 1, a plurality of client systems 10, each of which has a web

browser 11, OS(operating system) 13, a fingerprint acquisition module 15 and a fingerprint reader 17, are connected through the Internet 20 to an education server system 30 having a fingerprint authentication module 33 and a fingerprint DB 37. Fig. 2 shows a system that a plurality of the education servers 30' authenticate the clients 10 in connection with a
5 separate fingerprint authentication server 33'.

Fingerprint authentication procedure in such systems comprises the steps of fingerprint registration and fingerprint authentication.

The step of fingerprint registration is that students (hereinafter, referred to as "client") register his or her ID and fingerprint in the fingerprint DB 37 or 37' in advance. In
10 response to the request of the server 30 or 30', the client 10 enters his or her ID and provides fingerprint to the fingerprint reader 17. Then, the fingerprint acquisition module 15 converts the read fingerprint into fingerprint feature data, and transmits ID and the fingerprint feature data to the education sever 30 or 30'. Then, the education server 30 or 30' stores the ID and the fingerprint feature data in the fingerprint DB 37 or 37'. The
15 fingerprint input device is a hardware component possibly mounted on a keyboard, mouse or monitor.

The step of fingerprint authentication is a procedure that authenticates the client 10 by using the registered fingerprint feature data when the client 10 tries to log in the education server 30 or 30'. The client 10 enters his or her ID and provides fingerprint to the
20 fingerprint reader 17. Then, the fingerprint acquisition module 15 converts the input fingerprint into fingerprint feature data and transmits ID and the fingerprint feature data to the education sever 30 or 30'. The fingerprint authentication module 33 or the fingerprint authentication server 33' compares the transmitted fingerprint feature data with the data

stored in the fingerprint DB 37 or 37'. Accordingly, the client 10 is authenticated to log in the server 30 or 30' only when the transmitted fingerprint feature data matches the stored fingerprint feature data.

The above fingerprint authentication system, however, has a problem that whether
5 or not the client is faithful to the online lecture cannot be checked during the lecture because fingerprint authentication is made only once at the log-in time.

Disclosure of Invention

It is an object of the present invention to provide a method of attendance
10 management by using user authentication on an online education system, which can perform strict and effective attendance management in an online education system. To achieve the above object, there is provided a method of attendance management by using user authentication on an online education system, which is realized on the online system composed of a plurality of clients, a plurality of education servers having user DBs, and an
15 authentication server for authenticating the client to give him or her authority to be able to access the education servers by using biometric information (fingerprints, the iris, the retina, etc.), comprises the steps of: registering the client's biometric information in the authentication server; the client's logging in the education server through the authentication of the authentication server; and re-authenticating the client while the online lecture goes
20 on.

The third step above comprises the sub-steps of: the authentication server's requesting the client to be authenticated with his or her biometric information at random while the lecture goes on; storing in the user DB the interval time between an

authentication request point and the latest authenticated point, if the client does not respond to the authentication server's request; and adding up, after the lecture is over, the interval times that the client did not respond to the request for authentication and storing the result in the user DB.

5 Alternatively, the third step above may comprise the sub-steps of: the authentication server's requesting the client to be authenticated with his or her biometric information at random while the lecture goes on; storing in the user DB the interval time between an authentication request point and the next authentication request point, if the client does not respond to the authentication server's request; and adding up, after the lecture is over, the
10 interval times that the client did not respond to the request for authentication and storing the result in the user DB.

 Also, the third step above may comprise the sub-steps of: the authentication server's requesting the client to be authenticated with his or her biometric information at random while the lecture goes on; the authentication server's requesting the authentication
15 repeatedly for predetermined times, if the client does not respond to the authentication server's request; and disconnecting the client from the education server, if the client does not respond to the repeated request for predetermined times.

 In this invention, fingerprints may be preferably used as biometric information, and the authentication server can authenticate the client by matching the input fingerprint
20 feature data with the previously registered fingerprint feature data. As a matter of course, the iris, the retina, the voice and the face of the client can be also used as the biometric information.

Brief Description of Drawings

The above object, features and advantages of the present invention will become more apparent from the following detailed description when taken in conjunction with the accompanying drawings, in which:

5 Fig.1 shows an embodiment of a conventional fingerprint authentication system on the internet,

 Fig.2 shows another embodiment of a conventional fingerprint authentication system on the internet,

 Fig.3 is a process flow diagram depicting an embodiment of the method in
10 accordance with the present invention, and

 Fig.4 is a process flow diagram depicting another embodiment of the method in accordance with the present invention.

Preferred embodiment for Carrying out the Invention

15 The preferred embodiments in accordance with the present invention shall be detailed below, with reference to the associated drawings. Fig. 3 is a process flow diagram depicting an embodiment of the method in accordance with the present invention.

 The client 10 previously registers his or her own ID and fingerprint for authentication, in the fingerprint DB 37' of the fingerprint authentication server 33' [S1]. To
20 be more specific, when the client 10 enters his or her ID and provides fingerprint, the fingerprint acquisition module 15 converts the fingerprint into the fingerprint feature data and transmits the fingerprint feature data with the user ID to the education server 30 or 30'. Then the education server 30 or 30' transmits them to the fingerprint authentication module

33 or the fingerprint authentication server 33' so as to store them in the fingerprint DB 37 or 37'. The fingerprint reader 17, which is a hardware component to which the client can provide his or her fingerprint, may be mounted on the mouse, main body or monitor of a computer. It can be provided as a separate device.

5 The client 10 who registered fingerprint must log in the education server 30 or 30' through fingerprint authentication [S2]. More particularly, when the client 10 enters his or her ID and fingerprint, the fingerprint acquisition module 15 converts the fingerprint into the fingerprint feature data and transmits the fingerprint feature data with the user ID to the education server 30 or 30'. Then the education server 30 or 30' transmits them to the
10 fingerprint authentication module 33 or server 33', such that the fingerprint authentication module 33 or server 33' compares the transmitted data with the registered data in the fingerprint DB 37 or 37'. If the transmitted data matches the registered data, the client 10 is authenticated. The authenticated client 10 can now enter the education server 30 or 30' to attend an online lesson or lecture.

15 During the lecture, the education server 30 or 30' requests the client 10 to be authenticated again at random [S4], and the fingerprint authentication server 33' or the fingerprint authentication module 33 checks whether the client 10 responds to the request for authentication, thereby determining the interval time where the client 10 did not respond to.

20 There are two ways of determining the interval time where the client 10 did not respond to the request for authentication. The first way is that the interval between a certain authentication request point and the latest response point is regarded as the interval time. The second way is that the interval between a certain authentication request point and the

next request point is regarded as the interval time. The determined interval times are stored in the user DB [S5]. After the lecture is over, the determined interval times that the client did not respond to the result for authentication are added up and the result is stored in the user DB [S7].

5 Stored data may be used with various usages. For example, it may be used as record data in an education system, like a cyber-space school. It may be also used for providing supplementary lessons to the client 10 who was absent from the lecture, by counting the interval time that the client could not respond to the mid-lecture request for authentication during the lecture.

10 The following process may be proposed as another measures where the client 10 does not respond to the request for authentication which is made at random during the lecture. Fig. 4 shows the process. The education server 30 or 30' request the client to be fingerprint authenticated at any time during the lecture [S14]. When proper authentication is made, the lecture continues [S16]. Whereas authentication is not properly made, the
15 education server 30 or 30' repeats the request for fingerprint authentication for predetermined times. If proper authentication is still not made while the repeated requests have been made, the client 10 is disconnected compulsorily from the education server 30 or 30'.

 The present invention may be embodied in education systems not only on the
20 Internet, but on the other types of network. It is obvious to a person having ordinary skill in the art to which the invention pertains that this invention can be realized on the biometric information recognition systems which use the iris, the retina, the voice or the face as the biometric information.

The method of attendance management by using user authentication on an online education system in accordance with the present invention has the following effects.

First, the clients become faithful to the online education because the user authentication is made not only when the clients log in the server, but while the lecture goes
5 on.

Second, it may be used for providing supplementary lessons to the client who was absent from the lecture, by counting the interval times that the client could not respond to the mid-lecture request for authentication. It may also be used as record data in an education system, like a cyber-space school.

10 Third, attendance by proxy is impossible according to the present invention, unlike in the case of other methods of authentication, and the fingerprint authentication can be made more easily than any other authentication method, that is, instead of entering ID and password with the keyboard, the client's simple conduct of contacting his or her finger on the fingerprint input device mounted on the mouse or keyboard would be enough.

15 It will be appreciated by those of ordinary skill in the art that the invention can be embodied in other specific forms without departing from the spirit or essential character hereof. The present description is therefore considered in all respects to be illustrative and not restrictive. The scope of the invention is indicated by the appended claims, and all changes that come within the meaning and range of equivalents thereof are intended to be
20 embraced therein.

What Is Claimed Is:

1. A method of attendance management by using user authentication on an online education system which is realized on the online system composed of a plurality of clients, a plurality of education servers having user DBs and an authentication server for authenticating the clients to give him or her authority to be able to access the education servers by using biometric information, the method comprising the steps of:
 - a) registering the client's biometric information in the authentication server;
 - b) the client's logging in the education server through the authentication of the authentication server; and
 - 10 c) re-authenticating the client while the online lecture goes on.
2. The method according to claim 1, wherein the biometric information is the client's fingerprint.
3. The method according to claim 1, wherein the third step c) comprises the sub-steps of:
 - the authentication server's requesting the client to be authenticated *at random while*
 - 15 the lecture goes on;
 - storing in the user DB the interval time between an authentication request point and the latest authenticated point, if the client does not respond to the authentication server's request; and
 - adding up, after the lecture is over, the interval times that the client did not respond to
 - 20 the request for authentication and storing the result in the user DB.
4. The method according to claim 3, wherein the biometric information is the client's fingerprint.
5. The method according to claim 1, wherein the third step c) comprises the sub-steps of:

the authentication server's requesting the client to be authenticated at random while the lecture goes on;

storing in the user DB the interval time between an authentication request point and the next authentication request point, if the client does not respond to the authentication

5 server's request; and

adding up, after the lecture is over, the interval times that the client did not respond to the request for authentication and storing the result in the user DB.

6. The method according to claim 5, wherein the biometric information is the client's fingerprint.

10 7. The method according to claim 1, wherein the third step c) comprises the sub-steps of:

the authentication server's requesting the client to be authenticated at random while the lecture goes on;

the authentication server's requesting the authentication repeatedly for predetermined times, if the client does not respond to the authentication server's request; and

15 disconnecting the client from the education server, if the client did not respond to the repeated request for predetermined times.

8. The method according to claim 7, wherein the biometric information is the client's fingerprint.

DRAWINGS

Fig. 1

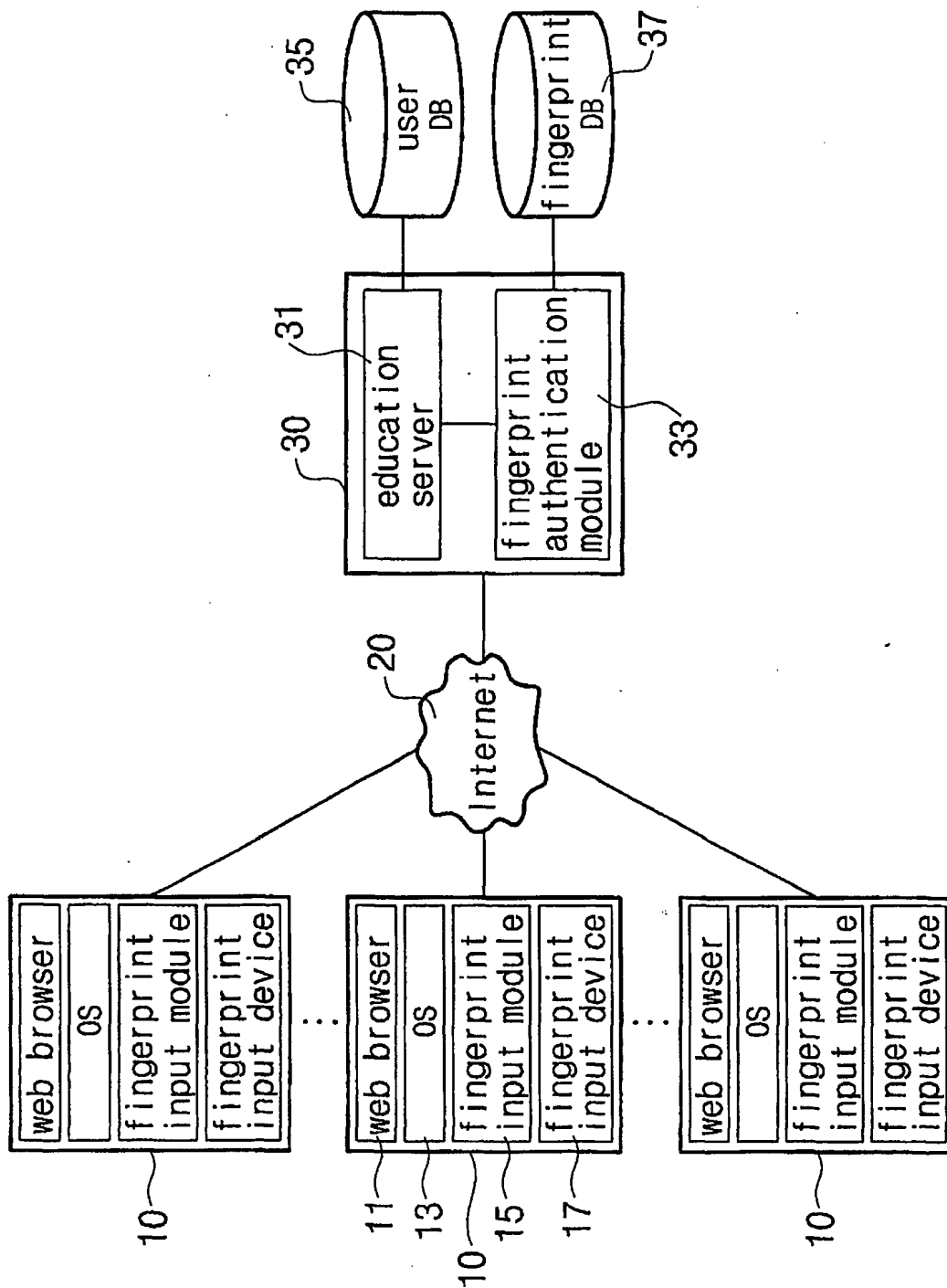


Fig. 2

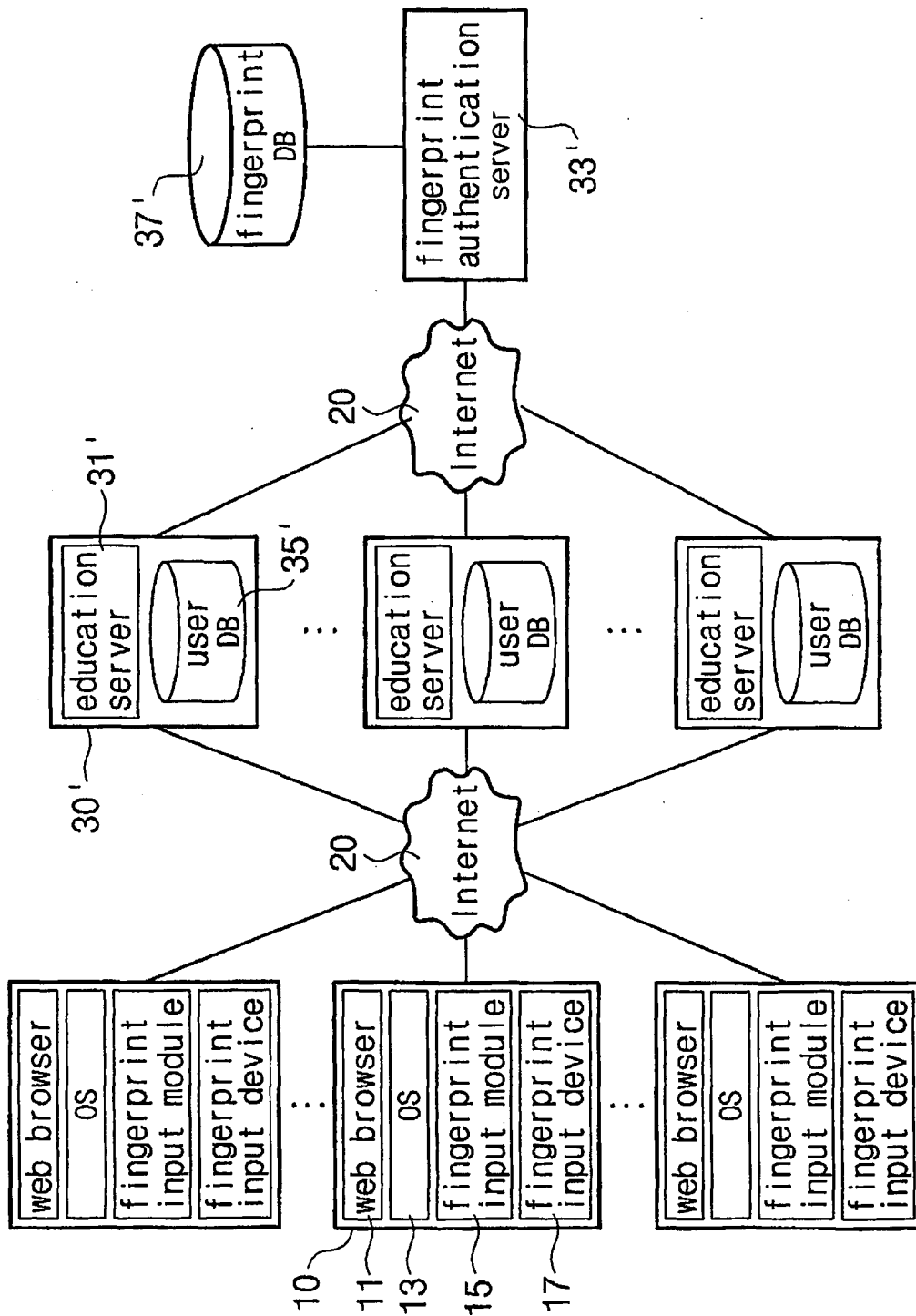


Fig. 3

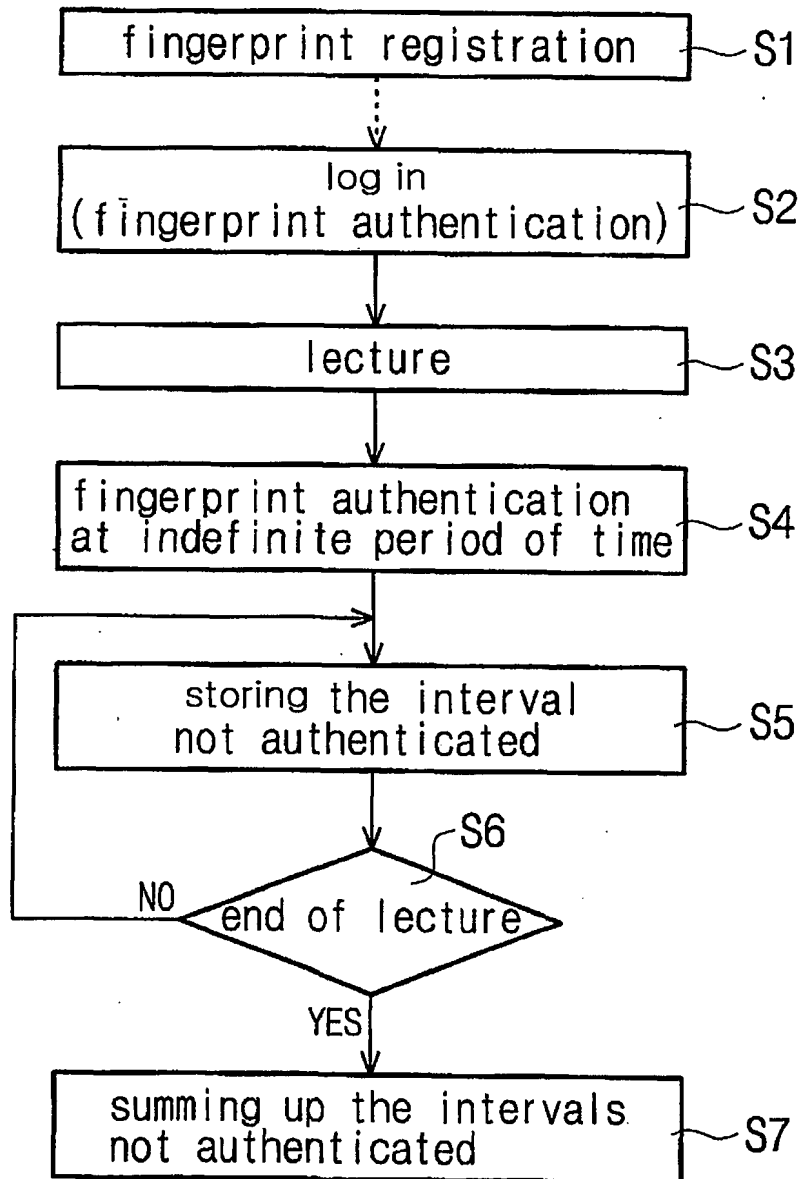
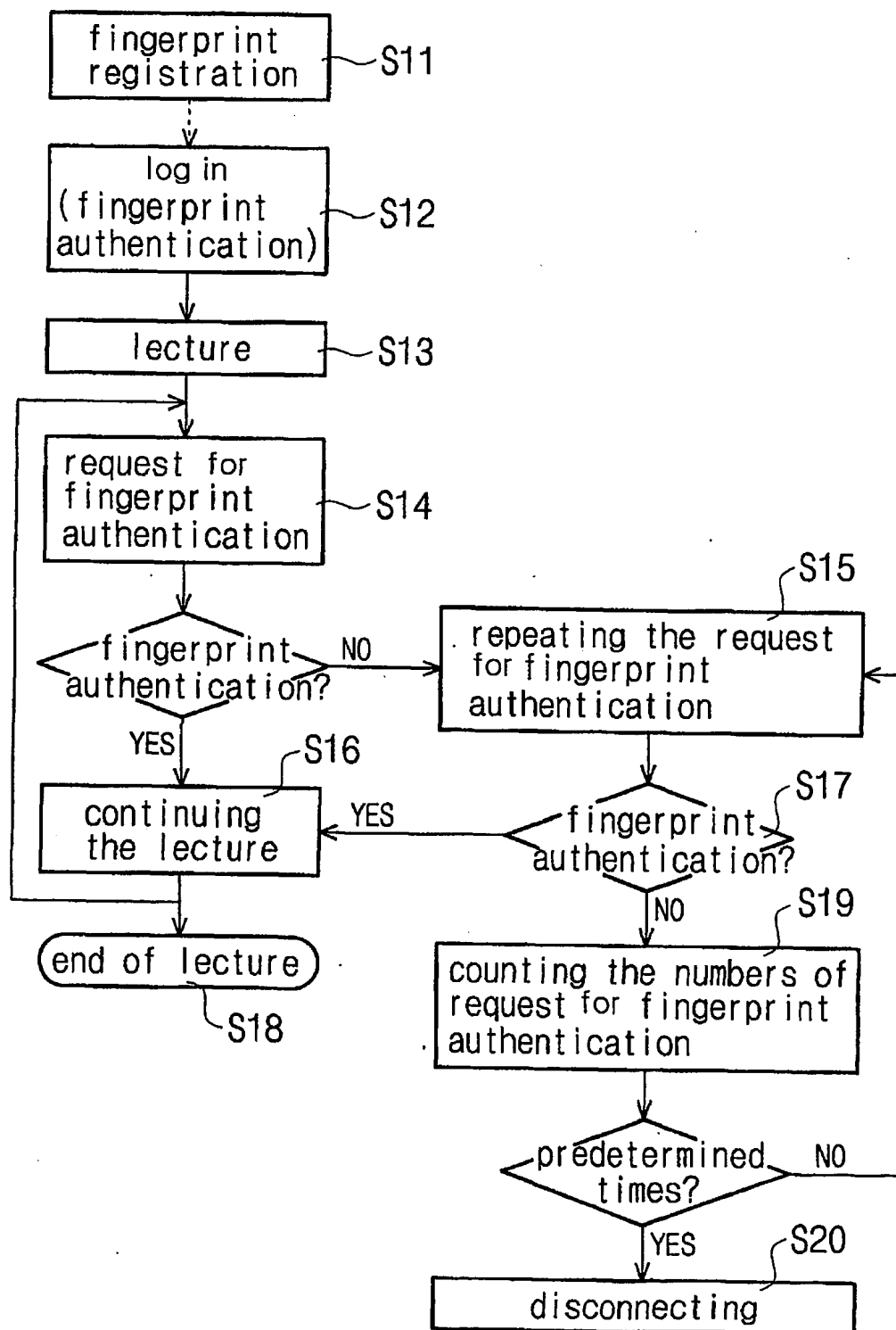


Fig. 4



INTERNATIONAL SEARCH REPORT

International application No.

PCT/KR02/01159

A. CLASSIFICATION OF SUBJECT MATTER**IPC7 G06F 17/60**

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC7 G06F 17/60

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Korean patents and applications for inventions since 1975 and Korean utility models and applications for utility models since 1975
Japanese utility models and applications for utility models since 1975

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
P,X	KR 2001-241389 Y1 (CHAOSMOS CO., LTD.) 12 OCTOBER 2001 the whole document	1-5
Y	KR 2000-37267 A (OBJECT VISION CO., LTD.) 5 JULY 2000 the whole document	1-5
Y	KR 2001-44537 A (LEE, WONG SEEK) 5 JUNE 2001 see the claim	1-5
Y	US 5930804 A (PHILIPS ELECTRONICS NA) 27 JULY 1999 see the abstract and drawings	1-5

☐ Further documents are listed in the continuation of Box C.☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search

14 OCTOBER 2002 (14.10.2002)

Date of mailing of the international search report

14 OCTOBER 2002 (14.10.2002)

Name and mailing address of the ISA/KR

Korean Intellectual Property Office
920 Dunsan-dong, Seo-gu, Daejeon 302-701,
Republic of Korea

Facsimile No. 82-42-472-7140

Authorized officer

KANG, Gab Youn

Telephone No. 82-42-481-5914



INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/KR02/01159

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
KR 2001-241389 Y1	12.10.2001	None	
KR 2000-37267 A	5.7.2000	None	
KR 2001-44537 A	5.6.2001	None	
US 5930804 A	27.7.1999	EP 923756 A1 JP 2000516746 T WO 9857247 A1	23.6.1999 12.12.2000 17.12.1998